

CONFERENCE MATRICES WITH MAXIMUM EXCESS AND TWO-INTERSECTION SETS

KOJI MOMIHARA* AND SHO SUDA†

ABSTRACT. A two-intersection set with parameters $(j; \alpha, \beta)$ for a block design is a j -subset of the point set of the design, which intersects every block in α or β points. In this paper, we show the existence of a two-intersection set with parameters $(2m^2 - m + 1; m^2 - m, m^2)$ for the block design obtained from translations of the set of nonzero squares in the finite field of order $q = 4m^2 + 1$. As an application, we give a construction of conference matrices with maximum excess based on the two-intersection sets.

1. INTRODUCTION

Let P be a set of v points and \mathcal{B} be a collection of b subsets of P , called *blocks*. We define $F = \{(p, B) \in P \times \mathcal{B} \mid p \in B\}$. Elements in F are called *flags*. The triple (P, \mathcal{B}, F) is called a *block design*. We say that $(\mathcal{B}, P, F^\perp)$ with $F^\perp = \{(B, p) \mid (p, B) \in F\}$ is the *dual* of (P, \mathcal{B}, F) . For convenience, we also say that the pair (P, \mathcal{B}) is a block design.

We consider a block design satisfying the following conditions: for each block $B \in \mathcal{B}$, there are exactly k elements $p \in P$ such that $p \in B$. Dually, for each point $p \in P$, there are exactly r blocks $B \in \mathcal{B}$ such that $p \in B$. Such a block design is called a *tactical configuration* or a *1-design*. It is clear that $vr = bk$. If for any two distinct points $a, b \in P$ the size of $\{B \in \mathcal{B} : a, b \in B\}$ is constant, say λ , (P, \mathcal{B}) is called a *2- (v, k, λ) design* or a *2-design* for short. In particular, if $v = b$, it is called *symmetric*.

Let (P, \mathcal{B}) be a block design and D be a j -subset of P . We say that D is a *two-intersection set with parameters $(j; \alpha, \beta)$ for (P, \mathcal{B})* if the set

$$\{|B \cap D| : B \in \mathcal{B}\}$$

contains exactly two numbers α and β . In this paper, we are interested in the existence of two-intersection sets and their applications. In particular, we consider a tactical configuration (P, \mathcal{B}) obtained from translations of the set of nonzero squares in the finite field \mathbb{F}_q of order $q \equiv 1 \pmod{4}$, and in Section 3, we prove that there exists a two-intersection set with parameters $(2m^2 - m + 1; m^2 - m, m^2)$ for (P, \mathcal{B}) if $q = 4m^2 + 1$.

Two-intersection sets have rich applications in algebraic combinatorics, in particular, for constructing strongly regular graphs and association schemes [3, 7, 17] while there was no paper uniformly treating two-intersection sets for block designs as far as the authors know. In Section 2, we explain some of such applications briefly. Furthermore, we find a new application of two-intersection sets for constructing conference matrices with maximum excess.

A *conference matrix of order n* is an $n \times n$ $(0, -1, 1)$ -matrix W with zero diagonal satisfying $WW^T = (n - 1)I$, where I is the $n \times n$ identity matrix. Conference matrices have been well-studied in relation to Hadamard matrices [8]. Let $E(W)$ denote the sum of all entries of W . We say that $E(W)$ is the *excess* of W . We will show the following upper bound for excess of conference matrices in Appendix.

Key words and phrases. conference matrix; excess; quadratic residue; two-intersection set.

MSC2010: 11T22; 11T23; 05B20; 05E30.

* Koji Momihara is supported by JSPS KAKENHI Grant Number (C)24540013.

† Sho Suda is supported by JSPS KAKENHI Grant Number 15K21075.

Proposition 1.1. *Let W be a conference matrix of order n and let k be an odd integer such that $k \leq \sqrt{n-1} < k+2$. Then, it holds that $E(W) \leq \frac{n(k^2+2k+n-1)}{2(k+1)}$ with equality if and only if either one of the following holds:*

- (i) $n-1$ is a square and $W\mathbf{1}_n = k\mathbf{1}_n$; or
- (ii) $n-1$ is a nonsquare and $W\mathbf{1}_n$ contains $k, k+2$ as its entries,

where $\mathbf{1}_n$ is the all one vector of length n .

The excess of Hadamard matrices and complex Hadamard matrices have been studied in [2, 6, 9, 10, 11, 12, 14, 16]. Note that regular conference matrices, that is conference matrices have the all-one vector as eigenvector, have the maximal excess, and see [5] for constructions of regular conference matrices. In this paper, we construct a conference matrix of order n with $n-1$ nonsquare with excess attaining the upper bound of Proposition 1.1 based on two-intersection sets obtained in Section 3. In particular, we will prove the following theorem.

Theorem 1.2. *For any prime power $q = p^r = 4m^2 + 1$ with p a prime congruent to 1 modulo 4, there exists a conference matrix of order $q+1$ with maximum excess attaining the bound of Proposition 1.1.*

2. TWO-INTERSECTION SETS AND THEIR APPLICATIONS

In this section, we consider two-intersection sets for tactical configurations. Let (P, \mathcal{B}) be a tactical configuration and D be a two-intersection set with parameters $(j; \alpha, \beta)$ for (P, \mathcal{B}) , i.e., $|D| = j$ and $\{|B \cap D| : B \in \mathcal{B}\} = \{\alpha, \beta\}$. It is clear that the complement of D is also a two-intersection set with parameters $(v-j; k-\alpha, k-\beta)$ for (P, \mathcal{B}) . Set

$$D_\alpha^\perp = \{B \in \mathcal{B} : |B \cap D| = \alpha\}, \quad D_\beta^\perp = \{B \in \mathcal{B} : |B \cap D| = \beta\}.$$

Then, $|D_\alpha^\perp| + |D_\beta^\perp| = b$ and $\alpha|D_\alpha^\perp| + \beta|D_\beta^\perp| = rj$. Hence, we have

$$|D_\alpha^\perp| = \frac{-\beta b + rj}{\alpha - \beta}, \quad |D_\beta^\perp| = b - \frac{-\beta b + rj}{\alpha - \beta}. \quad (2.1)$$

We say that each of D_α^\perp and D_β^\perp is the *dual* of D . Here, the following question naturally arises. Is the dual of D also a two-intersection set for the dual of (P, \mathcal{B}) ? The answer is no in general, but there is a class of block designs giving an affirmative answer.

Proposition 2.1. *Let (P, \mathcal{B}) be a $2-(v, k, \lambda)$ design and D be a two-intersection set with parameters $(j; \alpha, \beta)$ for (P, \mathcal{B}) . Then, the dual D_α^\perp is also a two-intersection set with parameters $(j^\perp; \alpha^\perp, \beta^\perp)$ for the dual of (P, \mathcal{B}) , where*

$$j^\perp = \frac{rj - \beta b}{\alpha - \beta}, \quad \alpha^\perp = \frac{\lambda j - \beta r}{\alpha - \beta}, \quad \beta^\perp = \frac{\lambda(j-1) + r - \beta r}{\alpha - \beta}.$$

Proof: Let N be the matrix whose rows and columns are labeled by the elements of P and \mathcal{B} , respectively, and entries are defined by

$$N_{p,B} = \begin{cases} 1 & \text{if } p \in B, \\ 0 & \text{if } p \notin B. \end{cases}$$

Let \mathbf{x} and \mathbf{y} be the $(0, 1)$ -vectors whose coordinates are labeled by the elements of P and \mathcal{B} , respectively, and entries are defined by

$$\mathbf{x}_p = \begin{cases} 1 & \text{if } p \in D, \\ 0 & \text{if } p \notin D, \end{cases} \quad \text{and} \quad \mathbf{y}_B = \begin{cases} 1 & \text{if } B \in D_\alpha^\perp, \\ 0 & \text{if } B \in D_\beta^\perp. \end{cases}$$

It is clear that

$$\mathbf{x}^T N = \alpha \mathbf{y}^T + \beta (\mathbf{1} - \mathbf{y})^T. \quad (2.2)$$

By multiplying both sides of (2.2) by N^T from right, we have

$$\mathbf{x}^T N N^T = (\alpha - \beta) \mathbf{y}^T N^T + \beta \mathbf{1}^T N^T.$$

Let I be the identity matrix of order v and J be the all-one matrix of order v . Since $N N^T = \lambda J + (r - \lambda)I$ and $\mathbf{1}^T N^T = r \mathbf{1}^T$, $\mathbf{y}^T N^T$ has exactly two entries $\alpha^\perp = (\lambda j - \beta r)/(\alpha - \beta)$ and $\beta^\perp = (\lambda(j - 1) + r - \beta r)/(\alpha - \beta)$. Furthermore, by multiplying both sides of (2.2) by $\mathbf{1}$ from right, we have

$$\mathbf{x}^T N \mathbf{1} = (\alpha - \beta) \mathbf{y}^T \mathbf{1} + \beta \mathbf{1}^T \mathbf{1}.$$

Since $\mathbf{x}^T N \mathbf{1} = r \mathbf{x}^T \mathbf{1} = rj$ and $\beta \mathbf{1}^T \mathbf{1} = \beta b$, we have $j^\perp = \mathbf{y}^T \mathbf{1} = (rj - \beta b)/(\alpha - \beta)$. Hence, the dual D_α^\perp is a two-intersection set for the dual of (P, \mathcal{B}) . \square

Remark 2.2. If (P, \mathcal{B}) is a 2-design, the parameter j is determined by the other parameters. Let $\mathcal{B}' = \{B \cap D \mid B \in \mathcal{B}\}$. Double-counting the number of pairs of distinct points of (D, \mathcal{B}') , we have $\binom{j}{2} \lambda = \binom{\alpha}{2} |D_\alpha^\perp| + \binom{\beta}{2} |D_\beta^\perp|$. Substituting (2.1), the parameter j is computable. In the language of design theory, (D, \mathcal{B}') is a *pairwise balanced design* with two block sizes.

Two-intersection sets have been studied in algebraic combinatorics in relation to strongly regular graphs and association schemes. Hereafter, we will assume that the reader is familiar with the theory of association schemes.

Example 2.3. (Projective two-intersection set) Let \mathbb{F}_q be the finite field of order q and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Let (P, \mathcal{B}) be the 2-design obtained from points and hyperplanes of the n -dimensional projective space $\text{PG}(n, q)$ over \mathbb{F}_q . Let D be a two-intersection set for (P, \mathcal{B}) . Define

$$C = \{xy : x \in D, y \in \mathbb{F}_q^*\}.$$

We consider the graph $\Gamma = (V, E)$ defined as $V = \mathbb{F}_q^{n+1}$ and $(x, y) \in E$ if and only if $x - y \in C$, which is called a *Cayley graph* on \mathbb{F}_q^{n+1} . The set C is called the *connection set* of Γ . It is known that this Cayley graph Γ forms a strongly regular graph [3, p. 134]. The set D is particularly called a *projective two-intersection set*. The existence of projective two-intersection sets has been well-studied in finite geometry.

Example 2.4. (Affine two-intersection set) Let (P, \mathcal{B}) be the 2-design obtained from points and hyperplanes of the n -dimensional affine space $\text{AG}(n, q)$ over \mathbb{F}_q . Let D be a two-intersection set for (P, \mathcal{B}) . We now assume that (P, \mathcal{B}) is a *residual* of the 2-design obtained from points and hyperplanes of $\text{PG}(n, q)$, i.e., P is the complement of a fixed hyperplane H of $\text{PG}(n, q)$ and the blocks $B \in \mathcal{B}$ are the restrictions of hyperplanes of $\text{PG}(n, q)$ to P . Then, we can regard D as a subset of the set of projective points of $\text{PG}(n, q)$. Then, the Cayley graphs on \mathbb{F}_q^{n+1} with connection sets

$$C_1 = \{xy : x \in D, y \in \mathbb{F}_q^*\}, C_2 = \{xy : x \in P \setminus D, y \in \mathbb{F}_q^*\}, C_3 = \{xy : x \in H, y \in \mathbb{F}_q^*\}$$

partition the complete graph on $V = \mathbb{F}_q^{n+1}$. In particular, this partition forms a 3-class association scheme [7]. The set D is called an *affine two-intersection set*. A first infinite family of affine two-intersection sets was recently found in [4, 7].

Example 2.5. (Relative 2-design) Let (P, \mathcal{B}) be a symmetric 2-design. Assume that there exists a two-intersection set D for (P, \mathcal{B}) satisfying $|D| = k$ and $D \notin \mathcal{B}$. Then, (P, \mathcal{B}) forms a tight relative 2-design with respect to D in the Johnson association scheme $J(v, k)$. Some constructions and all possible parameters with $v \leq 100$ were given in [17]. All the examples with $v \leq 100$ have the structure of coherent configurations.

We now give a new application of two-intersection sets for tactical configurations obtained from quadratic residues of finite fields. Let $q \equiv 1 \pmod{4}$ be a prime power and S be the set of nonzero squares of \mathbb{F}_q . Set $P = \mathbb{F}_q$ and

$$\mathcal{B} = \{\{x + a : x \in S\} : a \in \mathbb{F}_q\}. \quad (2.3)$$

Then, (P, \mathcal{B}) is a tactical configuration with $v = b = q$, $k = r = (q - 1)/2$. Note that (P, \mathcal{B}) does not form a 2-design. The set S is called the *Paley partial difference set*, which satisfies that the list $\{x - y : x, y \in S, x \neq y\}$ covers every element of S (resp. $\mathbb{F}_q^* \setminus S$) exactly $(q - 5)/4$ times (resp. $(q - 1)/4$ times). It is well-known that the Cayley graph on \mathbb{F}_q with connection set S forms a strongly regular graph. The Paley partial difference sets also have an application for constructing conference matrices. Let M be a $q \times q$ $(0, 1, -1)$ -matrix whose rows and columns are labeled by the elements of \mathbb{F}_q and entries are defined by

$$M_{i,j} = \begin{cases} 0 & \text{if } j - i = 0, \\ 1 & \text{if } j - i \in S, \\ -1 & \text{if } j - i \in \mathbb{F}_q^* \setminus S. \end{cases}$$

Define

$$W = \begin{pmatrix} 0 & \mathbf{1}_q^T \\ \mathbf{1}_q & -M \end{pmatrix}. \quad (2.4)$$

Then, W forms a conference matrix. We construct a conference matrix with maximum excess by switching the signs of some rows and columns of W .

Theorem 2.6. *Let $q = 4m^2 + 1$ be a prime power and (P, \mathcal{B}) be the block design defined in (2.3). Assume that there is a two-intersection set with parameters $(2m^2 - m + 1; m^2 - m, m^2)$ for (P, \mathcal{B}) . Then, there exists a conference matrix W' of order $q + 1$ such that $W'\mathbf{1}_{q+1}$ has entries $2m - 1$ and $2m + 1$.*

Proof: Let D be the assumed two-intersection set and W be the conference matrix defined in (2.4). Set $\alpha = m^2 - m$ and $\beta = m^2$. Multiply by -1 the columns indexed by the elements of D of $\begin{pmatrix} \mathbf{1}_q^T \\ -M \end{pmatrix}$. Denote the resulting matrix by $\begin{pmatrix} \mathbf{b}^T \\ M' \end{pmatrix}$. Then, multiply by -1 the rows indexed by the elements of D_α^\perp of $\begin{pmatrix} \mathbf{1}_q & M' \end{pmatrix}$. Denote the resulting matrix by $\begin{pmatrix} \mathbf{c} & M'' \end{pmatrix}$. Then, $W' = \begin{pmatrix} 0 & \mathbf{b}^T \\ \mathbf{c} & M'' \end{pmatrix}$ is the desired conference matrix.

It is clear that $\mathbf{b}^T \mathbf{1}_q = 2m - 1$ by the assumption that $|D| = 2m^2 - m + 1$. Furthermore, since $(\alpha, \beta) = (m^2 - m, m^2)$, we have

$$\left(\begin{pmatrix} \mathbf{1}_q & M' \end{pmatrix} \mathbf{1}_{q+1} \right)_i = \begin{cases} 2m - 1 & \text{if } i \in D_\beta^\perp \text{ and } i \notin D, \\ 2m + 1 & \text{if } i \in D_\beta^\perp \text{ and } i \in D, \\ -2m - 1 & \text{if } i \in D_\alpha^\perp \text{ and } i \notin D, \\ -2m + 1 & \text{if } i \in D_\alpha^\perp \text{ and } i \in D. \end{cases}$$

Hence, $W'\mathbf{1}_{q+1}$ has entries $2m - 1, 2m + 1$. □

In the next section, we will construct two-intersection sets satisfying the condition of Theorem 2.6. Then, Theorem 1.2 immediately follows by Proposition 1.1.

3. CONSTRUCTION OF TWO-INTERSECTION SETS

3.1. Preliminary on characters of finite fields. In this section, we will assume that the reader is familiar with the basic theory of characters of finite fields.

For a positive integer m , set $\zeta_m = \exp \frac{2\pi\sqrt{-1}}{m}$. Let $q = p^r$ be a prime power with p a prime. For a multiplicative character χ and the canonical additive character ψ of \mathbb{F}_q , we define the *Gauss sum* by

$$G_q(\chi) = \sum_{x \in \mathbb{F}_q^*} \chi(x) \psi(x) \in \mathbb{Z}[\zeta_{q-1}, \zeta_p].$$

We list a few basic properties of Gauss sums below:

- (i) $G_q(\chi) \overline{G_q(\chi)} = q$ if χ is nontrivial;

- (ii) $G_q(\chi^{-1}) = \chi(-1)\overline{G_q(\chi)}$;
- (iii) $G_q(\chi) = -1$ if χ is trivial.

Let ω be a primitive element of \mathbb{F}_q and k be a positive integer dividing $q - 1$. For $0 \leq i \leq k - 1$ we set $C_i^{(k,q)} = \omega^i C$, where C is the multiplicative subgroup of index k of \mathbb{F}_q^* . By the orthogonality of characters, the sums $\psi(C_i^{(k,q)}) = \sum_{x \in C_i^{(k,q)}} \psi(x)$, $0 \leq i \leq k - 1$, so-called *Gauss periods*, can be expressed as a linear combination of Gauss sums:

$$\psi(C_i^{(k,q)}) = \frac{1}{k} \sum_{j=0}^{k-1} G_q(\chi^j) \chi^{-j}(\omega^i), \quad 0 \leq i \leq k - 1, \quad (3.1)$$

where χ is a multiplicative character of order k of \mathbb{F}_q . For example, if $k = 2$, we have

$$\psi(C_i^{(2,q)}) = \frac{-1 + (-1)^i G_q(\eta)}{2}, \quad 0 \leq i \leq 1, \quad (3.2)$$

where η is the quadratic character of \mathbb{F}_q . In particular, the quadratic Gauss sum is explicitly computable.

Theorem 3.1. [13, Theorem 5.15] *Let $q = p^s$ be a prime power with p a prime and η be the quadratic character of \mathbb{F}_q . Then,*

$$G_q(\eta) = \begin{cases} (-1)^{s-1} q^{1/2} & \text{if } p \equiv 1 \pmod{4}, \\ (-1)^{s-1} \zeta_4^s q^{1/2} & \text{if } p \equiv 3 \pmod{4}. \end{cases} \quad (3.3)$$

Furthermore, we need to define *Jacobi sums*. We extend the domain of multiplicative characters χ of \mathbb{F}_q to all elements of \mathbb{F}_q by setting $\chi(0) = 1$ or $\chi(0) = 0$ depending on whether χ is trivial or not. For multiplicative characters χ_1 and χ_2 of \mathbb{F}_q , define

$$J(\chi_1, \chi_2) = \sum_{x \in \mathbb{F}_q} \chi_1(x) \chi_2(1 - x) \in \mathbb{Z}[\zeta_{q-1}].$$

In this paper, we treat Jacobi sums $J(\chi_1, \chi_2)$ with χ_1 the quadratic character and χ_2 a multiplicative character of order 4 of \mathbb{F}_q .

Lemma 3.2. ([15]) *Let $q \equiv 1 \pmod{4}$ be a prime power. Let η be the quadratic character and χ a multiplicative character of order 4 of \mathbb{F}_q . Put $J(\eta, \chi) = a + b\zeta_4 \in \mathbb{Z}[\zeta_4]$. Then,*

- (i) $a \equiv -1 \pmod{4}$ if $q \equiv 1 \pmod{8}$,
- (ii) $a \equiv 1 \pmod{4}$ if $q \equiv 5 \pmod{8}$.

Conversely, for any prime power $q = p^r = a^2 + b^2 \equiv 1 \pmod{4}$ with $p \equiv 1 \pmod{4}$ a prime satisfying (i) or (ii) above and $\gcd(a, q) = 1$, it holds that $J(\eta, \chi) = a + b\zeta_4$, where the sign of b is ambiguously determined. If $p \equiv 3 \pmod{4}$, r is even and $J(\eta, \chi) = a$.

In this paper, we do not need to care about the signs of a, b .

We will use the following formula on Jacobi sums in the next section.

Proposition 3.3. ([13, Exercise 5.60]) *For any $a, b \in \mathbb{F}_q^*$ and a multiplicative character χ of \mathbb{F}_q , it holds that*

$$\sum_{x \in \mathbb{F}_q} \chi(ax^n + b) = \chi(b) \sum_{j=1}^{d-1} \chi'^{-j}(a) \chi'^j(-b) J(\chi'^j, \chi),$$

where χ' is a multiplicative character of order $d = \gcd(n, q - 1)$ of \mathbb{F}_q .

3.2. Construction. Let $q = p^r = 4m^2 + 1$ be a prime power with p a prime congruent to 1 modulo 4, and let ω be a primitive element of \mathbb{F}_{q^2} . Let χ_4 be a multiplicative character of order 4 of \mathbb{F}_{q^2} , and η and χ'_4 be multiplicative characters of order 2 and 4 of \mathbb{F}_q , respectively. Assume that $\chi_4(\omega) = \chi'_4(\omega^{q+1}) = \zeta_4$. By Lemma 3.2, there are $\epsilon, \delta \in \{-1, 1\}$ such that $J(\eta, \chi'_4) = \epsilon + 2m\delta\zeta_4$.

Let ℓ be an integer not divisible by $q+1$, and put $n = \omega^{\ell(q+1)}$ and $t = \omega^\ell + \omega^{\ell q}$. Fix $h \in \{0, 1, 2, 3\}$ and ℓ so that the following conditions are satisfied:

$$\chi'_4(n) = \zeta_4^{\frac{-\epsilon\delta+1}{2}+h}, \quad \chi'_4(n - t^2/4) = -\zeta_4^{\epsilon+2h}. \quad (3.4)$$

We will see in Remark 3.7 that such a pair $(h, \ell) \in \{0, 1, 2, 3\} \times \{0, 1, \dots, q^2 - 2\}$ always exists.

Theorem 3.4. *Let $q = p^r = 4m^2 + 1$ be a prime power with p a prime congruent to 1 modulo 4, and let ω be a primitive element of \mathbb{F}_{q^2} . Let h and ℓ be integers defined as above. Define*

$$D_{\ell, h} = \left\{ x \in \mathbb{F}_q \mid 1 + x\omega^\ell \in C_h^{(4, q^2)} \cup C_{h+1}^{(4, q^2)} \right\}.$$

Then, the set $\{|D_{\ell, h} \cap (C_0^{(2, q)} + s)| : s \in \mathbb{F}_q\}$ contains exactly two numbers $m^2 - m$ and m^2 , and $|D_{\ell, h}| = 2m^2 - m + 1$.

This theorem implies that $D_{\ell, h}$ is a two-intersection with parameters $(j; \alpha, \beta) = (2m^2 - m + 1; m^2 - m, m^2)$ for the block design (P, \mathcal{B}) defined in (2.3). We prove this theorem by a series of propositions below.

Proposition 3.5. *Let $q \equiv 1 \pmod{4}$ be a prime power and χ_4 be a multiplicative character of order 4 of \mathbb{F}_{q^2} . Let ω be a primitive element of \mathbb{F}_{q^2} . Put $n = \omega^{\ell(q+1)}$ and $t = \omega^\ell + \omega^{\ell q}$. Then,*

$$\sum_{x \in \mathbb{F}_q} \chi_4(1 + \omega^\ell x) = \chi'_4{}^3(n) \chi'_4{}^3(n - t^2/4) J(\eta, \chi'_4),$$

where η and χ'_4 are multiplicative characters of order 2 and 4 of \mathbb{F}_q such that $\chi_4(\omega) = \chi'_4(\omega^{q+1})$.

Proof: Let χ_8 be a multiplicative character of order 8 of \mathbb{F}_{q^2} such that $\chi_8^{q+1} = \chi_4$. Note that the restriction of χ_8 to \mathbb{F}_q is of order 4, which coincides with χ'_4 . In fact,

$$\chi'_4(\omega^{q+1}) = \chi_4(\omega) = \chi_8^{q+1}(\omega) = \chi_8(\omega^{q+1}).$$

Then, we have

$$\begin{aligned} \sum_{x \in \mathbb{F}_q} \chi_4(1 + \omega^\ell x) &= \sum_{x \in \mathbb{F}_q} \chi_8((1 + \omega^\ell x)^{q+1}) \\ &= \sum_{x \in \mathbb{F}_q} \chi'_4(1 + tx + nx^2) \\ &= \sum_{x \in \mathbb{F}_q} \chi'_4(nx^2 + 1 - t^2/(4n)). \end{aligned} \quad (3.5)$$

By Proposition 3.3, the summation (3.5) is reformulated as

$$\begin{aligned} \sum_{x \in \mathbb{F}_q} \chi'_4(nx^2 + 1 - t^2/(4n)) &= \eta(n) \chi'_4{}^3(1 - t^2/(4n)) J(\eta, \chi'_4) \\ &= \chi'_4{}^3(n) \chi'_4{}^3(n - t^2/4) J(\eta, \chi'_4). \end{aligned}$$

This completes the proof. \square

Proposition 3.6. *With the notations of Proposition 3.5, assume that ℓ is not divisible by $q+1$. Then, for any $s \in \mathbb{F}_q$,*

$$\sum_{x \in \mathbb{F}_q \setminus \{s\}} \chi_4(1 + \omega^\ell x) \eta(x - s) = \chi'_4{}^3(u) \chi'_4{}^3(n - t^2/4) J(\eta, \chi'_4) - \chi'_4(n),$$

where $u = 1 + ts + ns^2$.

Proof: Since the restriction of χ_4 to \mathbb{F}_q is of order 2, we have

$$\begin{aligned} \sum_{x \in \mathbb{F}_q \setminus \{s\}} \chi_4(1 + \omega^\ell x) \eta(x - s) &= \sum_{y \in \mathbb{F}_q^*} \chi_4(1 + \omega^\ell(y + s)) \chi_4^{-1}(y) \\ &= \sum_{y \in \mathbb{F}_q^*} \chi_4(y^{-1}(1 + \omega^\ell s) + \omega^\ell) \\ &= \sum_{y \in \mathbb{F}_q} \chi_4(y(1 + \omega^\ell s) + \omega^\ell) - \chi_4(\omega^\ell). \end{aligned} \quad (3.6)$$

Note that $\chi_4(\omega^\ell) = \chi'_4(n)$ and $1 + \omega^\ell s \neq 0$. Setting $u = (1 + \omega^\ell s)(1 + \omega^{\ell q} s) = 1 + ts + ns^2 (\neq 0)$ and $v = w^{\ell q}(1 + \omega^\ell s) + w^\ell(1 + \omega^{\ell q} s)$, we have

$$\begin{aligned} (3.6) &= \sum_{y \in \mathbb{F}_q} \chi_8((y(1 + \omega^\ell s) + \omega^\ell)^{q+1}) - \chi'_4(n) \\ &= \sum_{y \in \mathbb{F}_q} \chi'_4(uy^2 + vy + n) - \chi'_4(n) \\ &= \sum_{y \in \mathbb{F}_q} \chi'_4(uy^2 + n - v^2/(4u)) - \chi'_4(n). \end{aligned} \quad (3.7)$$

By Proposition 3.3, the summation of the left hand side of (3.7) is reformulated as

$$\sum_{x \in \mathbb{F}_q} \chi'_4(ux^2 + n - v^2/(4u)) = \eta(u) \chi_4'^3(n - v^2/(4u)) J(\eta, \chi'_4).$$

Noting that $n - v^2/(4u) = (4n - t^2)/(4u)$, we obtain

$$(3.7) = \chi_4'^3(u) \chi_4'^3(n - t^2/4) J(\eta, \chi'_4) - \chi'_4(n).$$

This completes the proof. \square

We are now ready for proving Theorem 3.4.

Proof of Theorem 3.4: The characteristic functions of $C_0^{(2,q)}$ and $C_h^{(4,q^2)} \cup C_{h+1}^{(4,q^2)}$ are, respectively, given as

$$g(x) = \frac{1}{2}(\eta(x) + 1), \quad x \in \mathbb{F}_q^*,$$

and

$$f(x) = \frac{1}{4} \sum_{j=h, h+1}^3 \sum_{i=0}^3 \zeta_4^{-ji} \chi_4^i(x), \quad x \in \mathbb{F}_{q^2}^*.$$

The size N_s of the set $D_{\ell, h} \cap (C_0^{(2,q)} + s)$ is expressed as

$$\sum_{x \in \mathbb{F}_q \setminus \{s\}} f(1 + \omega^\ell x) g(x - s).$$

By the definitions of $g(x)$ and $f(x)$, we have

$$\begin{aligned} N_s &= \frac{1}{8} \sum_{x \in \mathbb{F}_q \setminus \{s\}} (\eta(x - s) + 1) \left(\sum_{j=h, h+1}^3 \sum_{i=0}^3 \zeta_4^{-ji} \chi_4^i(1 + \omega^\ell x) \right) \\ &= \frac{1}{8} \sum_{x \in \mathbb{F}_q \setminus \{s\}} (\eta(x - s) + 1) \left(2 + \zeta_4^{-h}(1 - \zeta_4) \chi_4(1 + \omega^\ell x) + \zeta_4^{-3h}(1 + \zeta_4) \chi_4^3(1 + \omega^\ell x) \right). \end{aligned} \quad (3.8)$$

Let $N_{s,1} = \sum_{x \in \mathbb{F}_q \setminus \{s\}} \chi_4(1 + \omega^\ell x)$ and $N_{s,2} = \sum_{x \in \mathbb{F}_q \setminus \{s\}} \chi_4(1 + \omega^\ell x) \eta(x - s)$. Then,

$$(3.8) = \frac{1}{8} \left(2q - 2 + \zeta_4^{-h}(1 - \zeta_4)(N_{s,1} + N_{s,2}) + \overline{\zeta_4^{-h}(1 - \zeta_4)(N_{s,1} + N_{s,2})} \right). \quad (3.9)$$

By Propositions 3.5 and 3.6, we have

$$N_{s,1} + N_{s,2} = (\chi'_4{}^3(n) + \chi'_4{}^3(u))\chi'_4{}^3(n - t^2/4)J(\eta, \chi'_4) - (\chi'_4(n) + \chi'_4(u)). \quad (3.10)$$

Here, we used $\chi_4(1 + \omega^\ell s) = \chi'_4(u)$. Substituting $\chi'_4(n) = \zeta_4^{\frac{-\epsilon\delta+1}{2}+h}$, $\chi'_4(n - t^2/4) = -\zeta_4^{\epsilon+2h}$ and $J(\eta, \chi'_4) = \epsilon + 2m\delta\zeta_4$ into (3.10) and continuing from (3.9), we have

$$N_s = \begin{cases} m^2 - m & \text{if } \epsilon\delta = -1 \text{ and } \chi'_4(u) \in \{\zeta_4^{h+1}, \zeta_4^{h+2}\} \\ & \text{or } \epsilon\delta = 1 \text{ and } \chi'_4(u) \in \{\zeta_4^h, \zeta_4^{h+3}\}, \\ m^2 & \text{if } \epsilon\delta = -1 \text{ and } \chi'_4(u) \in \{\zeta_4^h, \zeta_4^{h+3}\} \\ & \text{or } \epsilon\delta = 1 \text{ and } \chi'_4(u) \in \{\zeta_4^{h+1}, \zeta_4^{h+2}\}. \end{cases} \quad (3.11)$$

Thus, N_s takes exactly two values according to s .

Next, we compute the size of $D_{\ell,h}$:

$$|D_{\ell,h}| = \sum_{x \in \mathbb{F}_q} f(1 + x\omega^\ell) = \frac{1}{4} \sum_{x \in \mathbb{F}_q} \left(2 + \zeta_4^{-h}(1 - \zeta_4)\chi_4(1 + \omega^\ell x) + \zeta_4^{-3h}(1 + \zeta_4)\chi_4^3(1 + \omega^\ell x) \right). \quad (3.12)$$

By Proposition 3.5, we have

$$\sum_{x \in \mathbb{F}_q} \chi_4(1 + \omega^\ell x) = \chi'_4{}^3(n)\chi'_4{}^3(n - t^2/4)J(\eta, \chi'_4). \quad (3.13)$$

Substituting $\chi'_4(n) = \zeta_4^{\frac{-\epsilon\delta+1}{2}+h}$, $\chi'_4(n - t^2/4) = -\zeta_4^{\epsilon+2h}$ and $J(\eta, \chi'_4) = \epsilon + 2m\delta\zeta_4$ into (3.13) and continuing from (3.12), we have $|D_{\ell,h}| = 2m^2 - m + 1$. \square

Remark 3.7. In this remark, we show that there exists a pair $(h, \ell) \in \{0, 1, 2, 3\} \times \{0, 1, \dots, q^2 - 2\}$ satisfying the condition (3.4), i.e., the set

$$\left\{ (h, \ell) : (q+1) \nmid \ell, \chi'_4(n) = \zeta_4^{\frac{-\epsilon\delta+1}{2}+h}, \chi'_4(n - t^2/4) = -\zeta_4^{\epsilon+2h} \right\}$$

is nonempty. Let $\text{Tr}_{q^2/q}$ be the trace function from \mathbb{F}_{q^2} to \mathbb{F}_q . Note that $n - t^2/4 = -(\omega^\ell - \omega^{\ell q})^2/4 = -\omega^{-(q+1)}\text{Tr}_{q^2/q}(\omega^{\ell+\frac{q+1}{2}})^2/4$ is a nonsquare in \mathbb{F}_q . Hence,

$$\chi'_4(n - t^2/4) = \zeta_4^{-1}\eta(2\omega^{\frac{q-1}{4}}\text{Tr}_{q^2/q}(\omega^{\ell+\frac{q+1}{2}})).$$

Given $\epsilon, \delta \in \{-1, 1\}$, set h so that $\frac{-\epsilon\delta+1}{2}+h$ is odd, say, $2d+1$. This is valid whenever ℓ is odd since $\chi'_4(n) = \chi_4(\omega^\ell) = \zeta_4^{\frac{-\epsilon\delta+1}{2}+h}$. Then, the condition $(q+1) \nmid \ell$ is automatically satisfied. Furthermore, the condition $\chi'_4(n - t^2/4) = -\zeta_4^{\epsilon+2h}$ is equivalent to that

$$\eta(2\omega^{\frac{q-1}{4}}\text{Tr}_{q^2/q}(\omega^{\ell+\frac{q+1}{2}})) = -\zeta_4^{\epsilon+2h+1} = -\zeta_4^{\epsilon+2(2d+1-\frac{-\epsilon\delta+1}{2})+1} = \zeta_4^{\epsilon(1+\delta)}.$$

Therefore, it is enough to see that each of the sets

$$T_i = \left\{ \omega^\ell \in C_1^{(2,q^2)} \mid \text{Tr}_{q^2/q}(\omega^{\ell+\frac{q+1}{2}}) \in C_i^{(2,q)} \right\}, \quad i = 0, 1,$$

is nonempty. The size of each T_i is given by

$$\frac{1}{q} \sum_{a \in \mathbb{F}_q} \sum_{x \in C_1^{(2,q^2)}} \sum_{b \in C_i^{(2,q)}} \zeta_p^{\text{Tr}_q(a(\text{Tr}_{q^2/q}(x\omega^{\frac{q+1}{2}})-b))}, \quad (3.14)$$

where Tr_q is the trace function from \mathbb{F}_q to the prime field of \mathbb{F}_q . Let ψ and ψ' be the canonical additive characters of \mathbb{F}_{q^2} and \mathbb{F}_q , respectively. Then,

$$\begin{aligned} (3.14) &= \frac{1}{q} \sum_{a \in \mathbb{F}_q} \sum_{x \in C_1^{(2,q^2)}} \sum_{b \in C_i^{(2,q)}} \psi(ax\omega^{\frac{q+1}{2}}) \psi'(-ab) \\ &= \frac{1}{q} \sum_{a \in \mathbb{F}_q^*} \sum_{x \in C_1^{(2,q^2)}} \sum_{b \in C_i^{(2,q)}} \psi(ax\omega^{\frac{q+1}{2}}) \psi'(-ab) + \frac{(q-1)(q^2-1)}{4q}. \end{aligned} \quad (3.15)$$

Note that $\mathbb{F}_q^* \subset C_0^{(2,q^2)}$. Then, by (3.2) and (3.3), we have

$$\begin{aligned} (3.15) &= -\frac{q-1}{2q} \sum_{x \in C_1^{(2,q^2)}} \psi(x\omega^{\frac{q+1}{2}}) + \frac{(q-1)(q^2-1)}{4q} \\ &= -\frac{q-1}{2q} \left(\frac{-1 + G_{q^2}(\eta)}{2} \right) + \frac{(q-1)(q^2-1)}{4q} = \frac{q^2-1}{4}. \end{aligned}$$

Hence, each T_i is nonempty.

Remark 3.8. In this remark, we see that the dual of $D_{\ell,h}$ is also a two intersection set with parameters $(2m^2 - m; m^2 - m, m^2)$ for the block design obtained from translations of the set of “non-squares” in \mathbb{F}_q but not for (P, \mathcal{B}) . Let $D_{\ell,h}$ be the set defined in Theorem 3.4. Let $D_\alpha^\perp = \{s \in \mathbb{F}_q : |D_{\ell,h} \cap (C_0^{(2,q)} + s)| = m^2 - m\}$ and $D_\beta^\perp = \{s \in \mathbb{F}_q : |D_{\ell,h} \cap (C_0^{(2,q)} + s)| = m^2\}$. It is clear that $|D_\alpha^\perp| = 2m^2 - m$ by (2.1). By the definitions of u and χ'_4 , (3.11) is reformulated as

$$N_s = \begin{cases} m^2 - m & \text{if } s \in D_{\ell,h-\epsilon\delta}, \\ m^2 & \text{if } s \in D_{\ell,h+\epsilon\delta}. \end{cases}$$

This implies that $D_\alpha^\perp = D_{\ell,h-\epsilon\delta}$ and $D_\beta^\perp = D_{\ell,h+\epsilon\delta}$. Then, as in the proof of Theorem 3.4, we have

$$\begin{aligned} &|D_\alpha^\perp \cap (C_1^{(2,q)} + s)| \\ &= \frac{1}{8} \sum_{x \in \mathbb{F}_q \setminus \{s\}} (-\eta(x-s) + 1) \left(2 + \zeta_4^{-h+\epsilon\delta} (1 - \zeta_4) \chi_4(1 + \omega^\ell x) + \zeta_4^{-3h+3\epsilon\delta} (1 + \zeta_4) \chi_4^3(1 + \omega^\ell x) \right) \\ &= \frac{1}{8} \left(2q - 2 + \zeta_4^{-h+\epsilon\delta} (1 - \zeta_4) (N_{s,1} - N_{s,2}) + \overline{\zeta_4^{-h+\epsilon\delta} (1 - \zeta_4) (N_{s,1} - N_{s,2})} \right) \\ &= \begin{cases} m^2 - m & \text{if } s \in D_{\ell,h+2}, \\ m^2 & \text{if } s \in D_{\ell,h}. \end{cases} \end{aligned}$$

This implies that the dual of D forms a two-intersection set for the block design obtained from translations of $C_1^{(2,q)}$ in \mathbb{F}_q .

REFERENCES

- [1] B. Berndt, R. Evans, K.S. Williams, *Gauss and Jacobi Sums*, Wiley, 1997.
- [2] M.R. Best, The excess of Hadamard matrix, *Indagationes Math.* **80**, 357–361, (1977).
- [3] A.E. Brouwer, W.H. Haemers, *Spectra of Graphs*, Springer, New York, 2012.
- [4] J. De Beule, J. Demeyer, K. Metsch, M. Rodgers, A new family of tight sets in $\mathcal{Q}^+(5, q)$, *Des. Codes Cryptogr.* **78**, 655–678, (2016).
- [5] R. Craigen, Regular conference matrices and complex Hadamard matrices, *Utilitas Math.* **45**, 65–69, (1994).
- [6] N. Farmakis, S. Kounias, The excess of Hadamard matrices and optimal designs, *Discr. Math.* **67**, 165–176, (1987).
- [7] T. Feng, K. Momihara, Q. Xiang, Cameron-Liebler line classes with parameter $x = \frac{q^2-1}{2}$, *J. Combin. Theory Ser. A* **133**, 307–338, (2015).

- [8] Y.J. Ionin, H. Kharaghani, Balanced Generalized Weighing Matrices and Conference Matrices, in: C.J. Colbourn, J.H. Dinitz, (eds.) *The CRC Handbook of Combinatorial Designs, 2nd edn*, 306–313. Chapman & Hall/CRC Press, Boca Raton, FL, 2006.
- [9] H. Kharaghani, A infinite class of Hadamard matrices of maximal excess, *Discr. Math.* **89**, 307–312, (1991).
- [10] H. Kharaghani, J. Seberry, The excess of complex Hadamard matrices, *Graphs Combin.* **9**, 47–56, (1993).
- [11] C. Koukouvinos, S. Kounias, Construction of some Hadamard matrices with maximum excess, *Discr. Math.* **85**, 295–300, (1990).
- [12] C. Koukouvinos, J. Seberry, Hadamard matrices of order $\equiv 8 \pmod{16}$ with maximal excess, *Discr. Math.* **92**, 173–176, (1991).
- [13] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, 1997.
- [14] J. Seberry, Existence of SBIBD($4k^2, 2k^2 \pm k, k^2 \pm k$) and Hadamard matrices with maximal excess, *Austral. J. Combin.* **4**, 87–91, (1991).
- [15] T. Storer, *Cyclotomy and Difference Sets*, in: Lectures in Advanced Mathematics, Markham Publishing Company, 1967.
- [16] T. Xia, M. Xia, J. Seberry, Regular Hadamard matrix, maximum excess and SBIBD, *Austral. J. Combin.* **27**, 263–275, (2003).
- [17] Y. Zhu, Ei. Bannai, Et. Bannai, Tight relative 2-designs on two shells in Johnson association schemes, *Discr. Math.* **339**, 957–973, (2016).

APPENDIX: UPPER BOUNDS ON EXCESS OF CONFERENCE MATRICES

In this appendix, we prove Proposition 1.1.

Proposition 3.9. *Let W be a conference matrix of order n . Then $E(W) \leq n\sqrt{n-1}$ holds with equality if and only if $W\mathbf{1}_n = \sqrt{n-1}\mathbf{1}_n$.*

Proof: Write

$$W\mathbf{1}_n = (w_1, w_2, \dots, w_n)^T.$$

Then

$$\sum_{i=1}^n w_i^2 = (\mathbf{1}_n^T W^T)(W\mathbf{1}_n) = (n-1)\mathbf{1}_n^T \mathbf{1}_n = (n-1)n.$$

Thus by Cauchy-Schwartz inequality,

$$E(W) \leq |E(W)| \leq \sum_{i=1}^n |w_i| \leq \sqrt{\left(\sum_{i=1}^n w_i^2\right) \underbrace{(1^2 + \dots + 1^2)}_n} = n\sqrt{n-1}.$$

The equality holds if and only if w_i are all equal, that is $w_i = \sqrt{n-1}$ for each i . Thus, we obtain the assertion. \square

If the equality holds in Proposition 3.9, then $n-1$ must be a square. In the next proposition, we improve this upper bound when $n-1$ is a nonsquare.

Proposition 3.10. *Let W be a conference matrix of order n with $n-1$ a nonsquare. Let k be an odd integer such that $k \leq \sqrt{n-1} < k+2$. Then*

$$E(W) \leq \frac{n(k^2 + 2k + n - 1)}{2(k+1)}$$

with equality holds if and only if $W\mathbf{1}_n$ has entries $k, k+2$.

Proof: Write

$$W\mathbf{1}_n = (w_1, w_2, \dots, w_n)^T.$$

By the following equation

$$\sum_{i=1}^n (w_i - \sqrt{n-1})^2 = 2n(n-1) - 2\sqrt{n-1} \sum_{i=1}^n w_i,$$

the value $\sum_{i=1}^n w_i$ takes maximum if and only if the value $\sum_{i=1}^n (w_i - \sqrt{n-1})^2$ takes minimum. The latter occur only if each w_i is either k or $k+2$. Here, noting that the sum of entries in each row has the same parity with $n-1$, $w_i = k+1$ is impossible. In this case,

$$W\mathbf{1}_n = \begin{pmatrix} k\mathbf{1}_a \\ (k+2)\mathbf{1}_{n-a} \end{pmatrix},$$

and the number a of k in $W\mathbf{1}_n$ is determined as $a = \frac{n((k+2)^2 - (n-1))}{4(k+1)}$ by $\sum_{i=1}^n w_i^2 = n(n-1)$. Then

$$\begin{aligned} E(W) &= \sum_{i=1}^n w_i = \frac{1}{2\sqrt{n-1}}(2n(n-1) - \sum_{i=1}^n (w_i - \sqrt{n-1})^2) \\ &\leq n\sqrt{n-1} - \frac{1}{2\sqrt{n-1}}(a(k - \sqrt{n-1})^2 + (n-a)(k+2 - \sqrt{n-1})^2) = \frac{n(k^2 + 2k + n - 1)}{2(k+1)} \end{aligned}$$

with equality holds if and only if $W\mathbf{1}_n$ has only two entries $k, k+2$. \square

Combining Propositions 3.9 and 3.10, we have Proposition 1.1. Note that Propositions 3.9 and 3.10 are generalizable for excess of general *weighing matrices*.

* FACULTY OF EDUCATION, KUMAMOTO UNIVERSITY, 2-40-1 KUROKAMI, KUMAMOTO 860-8555, JAPAN
E-mail address: momihara@educ.kumamoto-u.ac.jp

† DEPARTMENT OF MATHEMATICS EDUCATION, AICHI UNIVERSITY OF EDUCATION, 1 HIROSAWA, IGAYA-CHO, KARIYA, AICHI 448-8542, JAPAN
E-mail address: suda@aecc.aichi-edu.ac.jp